WE CLAIM:

1. An encryption device for a telephone having a handset and a base unit, comprising:

a handset interface that receives analog output signals from the handset;

a first converter that converts the analog output signals into digital output signals;

an encryption processor comprising a compressor that compresses the digital output signals, a key manager that generates first key material for encrypting the digital output signals, an encryptor that encrypts the digital output signals based on the first key material, and a modulator that modulates the encrypted digital output signals;

a second converter that converts the encrypted digital output signals into encrypted analog output signals; and

a host interface that receives the encrypted analog output signals from the encryption processor, and forwards the encrypted analog output signals to the base unit.

2. The encryption device of claim 1, further comprising:

a human-machine interface coupled to the encryption processor via which a user of the encryption device can communicate with the encryption processor.

3. The encryption device of claim 1, further comprising:

a gain adjustment circuit coupled to the base unit interface that adjusts a signal level of the encrypted analog output signals.

4. The encryption device of claim 2, further comprising:

a gain adjustment circuit coupled to the base unit interface that adjusts a signal level of the encrypted analog output signals,

wherein the encryption processor receives from the human-machine interface a code that corresponds to the telephone, and wherein the gain adjustment circuit adjusts the signal level of the encrypted analog output signals based on the received code.

5. The encryption device of claim 1, further comprising:

a bypass control circuit that is coupled to the handset interface and to the base unit interface, via which the analog output signals can bypass the encryption processor.

6. The encryption device of claim 5, further comprising a human-machine interface via which a user of the device can cause the analog output signals to selectively bypass the encryption processor.

7. The encryption device of claim 1, further comprising:

a bias detect circuit coupled to the base unit interface; and

a microphone bias circuit coupled to the bias detect circuit and to the handset interface,

wherein the bias detect circuit detects a bias voltage polarity provided by the base unit interface, and directs the microphone bias circuit to provide the bias voltage polarity to the handset.

8. The encryption device of claim 1, wherein

the host interface receives analog input signals from the base unit;

the second converter converts the analog input signals into digital input signals;

the key manager generates second key material for decrypting the digital input signals;

the encryption processor comprises a demodulator that demodulates the digital input signals, a decryptor that decrypts the digital input signals based on the second key material, and a decompressor that decompresses the decrypted digital input signals;

the first converter converts the decrypted digital input signals into decrypted analog input signals; and

the handset interface receives the decrypted analog input signals from the decryption processor, and forwards the decrypted analog input signals to the handset.

9. The encryption device of claim 8, further comprising:

a second gain adjustment circuit coupled to the handset interface that adjusts a signal level of the decrypted analog input signals.

10. A decryption device for a telephone having a handset and a base unit, comprising:

a host interface that receives analog input signals from the base unit;

a first converter that converts the analog input signals into digital input signals;

a decryption processor comprising a demodulator that demodulates the digital input signals, a key manager that generates key material for decrypting the digital input signals, a decryptor that decrypts the digital input signals based on the key material, and a decompressor that decompresses the decrypted digital input signals;

a second converter that converts the decrypted digital input signals into decrypted analog input signals; and

a handset interface that receives the decrypted analog input signals from the decryption processor, and forwards the decrypted analog input signals to the handset.

11. The decryption device of claim 10, further comprising:

a human-machine interface coupled to the decryption processor via which a user of the decryption device can communicate with the decryption processor.

12. The decryption device of claim 10, further comprising:

a gain adjustment circuit coupled to the base unit interface that adjusts a signal level of the analog input signals.

13. The decryption device of claim 11, further comprising:

a gain adjustment circuit coupled to the base unit interface that adjusts a signal level of the analog input signals,

wherein the decryption processor receives from the human-machine interface a code that corresponds to the telephone, and wherein the gain adjustment circuit adjusts the signal level of the analog input signals based on the received code.

14. The decryption device of claim 10, further comprising:

a bypass control circuit that is coupled to the handset interface and to the base unit interface, via which the analog input signals can bypass the decryption processor.

15. The decryption device of claim 14, further comprising a human-machine interface via which a user of the device can cause the analog input signals to selectively bypass the decryption processor.

16. The decryption device of claim 10, further comprising:

a bias detect circuit coupled to the base unit interface; and

a microphone bias circuit coupled to the bias detect circuit and to the handset interface,

wherein the bias detect circuit detects a bias voltage polarity provided by the base unit interface, and directs the microphone bias circuit to provide the bias voltage polarity to the handset.

17. An encryption device for a telephone having a handset and a base unit, comprising:

a handset interface that receives output signals from the handset;

an encryption processor coupled to the handset interface that receives the output signals from the handset interface and encrypts the output signals by

generating a cryptographic session key,

defining a state vector having a vector length,

encrypting the state vector to produce a keystream using the cryptographic session key and a cryptographic block transformation corresponding to the vector length, and

combining the keystream with the output signals to produce encrypted output signals; and

a host interface coupled to the encryption processor that receives the encrypted output signals from the encryption processor, and forwards the encrypted output signals to the base unit.

18. The encryption device of claim 17, wherein the state vector includes a variable field, and wherein the encryption processor defines the state vector, at least in part, by incrementing a value of the variable field.

19. An encryption device for a telephone having a handset and a base unit, comprising:

a handset interface coupled to the handset;

a processor coupled to the handset interface having a memory for storing a set of security parameters; and

a host interface coupled to the processor and to the base unit,

wherein the processor transmits to a far-end telephone via the host interface a message containing a representation of the set of security parameters, receives from the far-end telephone via the host interface a message containing a selected security parameter selected from the set of security parameters, and establishes a secure session with the far-end telephone based on the selected security parameter.

20. An encryption device for a telephone having a handset and a base unit, comprising:

a handset interface coupled to the handset;

a processor coupled to the handset interface having a memory for storing a first set of security parameters; and

a host interface coupled to the processor and to the base unit,

wherein the processor receives from a far-end telephone via the host interface a message containing a representation of a second set of security parameters, determines whether a security parameter from the first set is compatible with a security parameter from the second set, and, if a security parameter from the first set is compatible with a security parameter from the second set, transmits to the far-end telephone via the host interface a message containing a representation of the compatible security parameter.